Department of Children's Services

HIPAA Companion Guide

Front Matter

Version 4010A1

September 2003 Draft Version

Disclaimer: Department of Children's Services (DCS) Companion Guides describe the technical interface environment with DCS, including connectivity requirements and protocols, and electronic interchange procedures. The Companion Guide documents are intended to be supplemental to and <u>NOT</u> a replacement for the standard Implementation Guide for each transaction set. Substantial effort has been taken to minimize any such conflicts or errors; however, DCS or its employees will not be liable or responsible for any errors or expenses resulting from the use of information in these documents. If you believe there is an error in any document, please notify the DCS Information Resources Division immediately.

Table of Contents

Article I.   Introduction

Section 1.01   Document Objective

This Companion Document describes the technical interface environment with DCS, including connectivity requirements and protocols, and electronic interchange procedures.

Section 1.02   Companion Guide Organization

The DCS HIPAA Companion Guide is organized into multiple documents that will be available on the DCS HIPAA website. Each HIPAA transaction conducted by DCS will have at least one associated companion guide available on the website. This distributed documentation method allows each DCS Trading Partner to access and download only the transactions that apply to their line of business instead of downloading the entire set of companion guides.

The following Companion Documents will be available.
   (a)   270 Eligibility Inquiry
   (b)   271 Eligibility Response
   (c)   276 Claim Status Request
   (d)   277 Claim Status Response
   (e)   278 Referral Certification and Authorization
   (f)   835 Claims Remittance Advice
   (g)   837(I & P) Health Care Claims

Section 1.03   Relationship to HIPAA Implementation Guides

The Companion Guide is intended to supplement the HIPAA Implementation Guides for each of the HIPAA transactions. The rules for the format, contents, and field values can be found in the Implementation Guides. The Companion Guide describes the technical interface environment with DCS, including connectivity requirements and protocols, and electronic interchange procedures. The Companion Guide also provides specific information on the fields and values required for transactions sent to or received from DCS.

The Companion Guide is intended to be supplemental to and NOT a replacement for the standard Implementation Guide for each transaction set. Based upon reporting circumstances, certain loops or data elements that are normally situational may become required. Some of these situational loops may not be included within the DCS

Companion Guide for a given transaction; however, requirements within the implementation guide must be followed when using different loops, segments and data elements. HIPAA required information must be met even if it's not part of the companion guide.

The information in the DCS documents is <u>not</u> intended to:

    a) Modify the definition, data condition, or use of any data element or segment in the standard Implementation Guides.

    b) Add any additional data elements or segments to the defined data set.

    c) Utilize any code or data values that are not valid in the standard Implementation Guides.

    d) Change the meaning or intent of any implementation specifications in the standard Implementation Guides.

Section 1.04   DCS Introduction

DCS is pleased to make available our Health Insurance Portability and Accountability Act (HIPAA) Companion Guide. These documents are the culmination of a long process and represent a significant milestone in our ongoing effort to adhere to the HIPAA transaction set requirements. HIPAA provides all healthcare entities a tremendous opportunity to realize many administrative and systemic benefits because it provides a national standard of transaction and code sets for the electronic exchange of healthcare information. DCS is committed to the implementation of HIPAA transaction sets within the DCS systems.

The purpose of this manual and accompanying documents is to provide information necessary to submit claims to DCS electronically. This manual is to be used in conjunction with the National Electronic Data Interchange Transaction Set Implementation Guides. The Implementation Guides can be obtained exclusively from the Washington Publishing Company by calling 1-800-972-4334 or are available for download on their web site at <u>www.wpc-edi.com/hipaa</u>. The Implementation Guides provide the majority of the HIPAA transaction and code set requirements, compared to the DCS Companion Guide, which only provide the supplemental requirements specific to DCS, as permitted within the structure of the HIPAA transaction sets. All DCS Trading Partners who submit claims electronically to DCS must adhere to the HIPAA Implementation Guide and the DCS Companion Guide requirements.

DCS filed an extension with the Centers for Medicare and Medicaid Services (CMS, formerly HCFA) in October 2002, thus delaying our mandatory implementation until October 16, 2003. DCS intends to implement all HIPAA transaction sets that are conducted as part of its Program. Updates to companion guide documents will be provided as they are developed.

HIPAA does not mandate the use of these transaction sets for the exchange of healthcare

data. Any provider may continue to submit paper claims and receive a paper remittance advice. However, if a provider elects to submit claims electronically and/or receive an electronic remittance advice, HIPAA does require the use of standard transactions and code sets.

In order to reach compliance with these Federal Regulations, DCS plans to procure Clearinghouse services for the purpose of submitting and receiving all HIPAA transactions on their behalf. The anticipated production implementation for all DCS HIPAA transactions and code sets standards via the Clearinghouse is April 1, 2004. DCS will continue to support the existing transaction formats until such implementation occurs. Additionally, non-standard HIPAA procedure codes will be allowed on claims/encounters with a date-of-service through December 31, 2003. This date was extended from October 15, 2003 by CMS on June 6, 2003.

DCS's companion guide uses the approved Addenda in our HIPAA Companion Guide. Additional changes may be required to bring our Companion Guide in line with our business needs. The underlying point is these documents are subject to change.

All comments, suggestions, and/or questions regarding the Companion Guide should be directed to:

State of Tennessee
Department of Children's Services
Attn: Wendy Van Sickle, Information Resources
14th Floor, Andrew Jackson Building
500 Deaderick Street
Nashville, TN 37242
Phone: (615) 253-1008

Section 1.05 Intended Users

The Companion Guide transaction documents are intended for the technical staff of the external entities that will be responsible for the electronic transaction/file exchanges. The Companion Guide is available to external entities (health plans, program contractors, providers, other state agencies, third party processors, and billing services) to clarify the information on HIPAA-compliant electronic interfaces with DCS.

Section 1.06 HIPAA Overview

The Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II) required the Department of Health and Human Services to establish national standards for electronic healthcare transactions and national identifiers for providers, health plans, and employers. HIPAA also addresses the security and privacy of health data. Adopting standards will eventually improve the

efficiency and effectiveness of the nation's healthcare system by encouraging the widespread use of electronic data interchange in healthcare. The intent of the law is that all electronic transactions, for which standards are specified, must be conducted according to the standards. These standards were not imposed by the law, but instead were developed by a process that included significant public and private sector input. Covered entities are required to accept these transmissions in the standard format in which they are sent and must not delay a transaction or adversely affect an entity that wants to conduct the transactions electronically.

Section 1.07   HIPAA Background

In the early 1990s, the first Bush Administration assembled an advisory group of healthcare industry leaders to discuss ways to reduce health care administrative costs across the nation. This group, which is now recognized as the Workgroup for Electronic Data Interchange (WEDI), recommended that Federal legislation be passed to implement a nationwide standard of transaction and code sets to be used by the healthcare industry. This law was entitled "The Health Insurance Portability and Accountability Act" and was enacted on August 21, 1996 under the Clinton Administration.

HIPAA requires several provisions. One provision, already in effect, deals with the portability of health insurance coverage during a change in employment, and primarily affects employers and health insurers. Another provision, often referred to as "Administrative Simplification", deals with the implementation of healthcare standards, of which transaction and code sets are but one part. The following standard transactions will be used by DCS:

(a) Eligibility Inquiry and Response: HIPAA mandates X12 Version 4010A1 of the 270/271 Eligibility and Benefit Inquiry and Response EDI Transactions for this purpose.

(b) Claim Status Inquiry and Response: HIPAA mandates X12 Version 4010A1 of the 276/277 Claim Status Inquiry and Response EDI Transaction for this purpose.

(c) Referral Certification and Authorization: HIPAA mandates X12 Version 4010A1 of the 278 Health Care Service Review EDI Transaction for this purpose.

(d) Claim Payment and Remittance Advice: HIPAA mandates X12 Version 4010A1 of the 835 Healthcare Claim Payment/Advice EDI Transaction for this purpose.

(e) Claims and Encounters: HIPAA mandates the X12 Version 4010A1 of the 837I for Institutional transactions, and 837P for Professional transactions.

HIPAA also requires the standardization of code sets. Any coded field or data element contained in a HIPAA transaction must adhere to a national set of code set values, including medical services and diagnoses. As such, DCS is required to discontinue the use of local codes, most notably the Level III HCPCS (procedure codes), which are

specific to DCS. Non-standard local codes will be allowed on claims/encounters with a date-of-service through December 31, 2003. This date was extended from October 15, 2003 by CMS on June 6, 2003.

Section 1.08   Additional HIPAA Requirements

In addition to the transaction and code set aspects, there are other requirements of the "Administrative Simplification" provision of HIPAA:

(a) <u>Privacy</u>: Standards must be adopted by all health plans, clearinghouses, and providers that ensure the protection and appropriate disclosure of individually identifiable health information. The final rule had a mandatory implementation of April 14, 2003.

(b) <u>Security</u>: Standards must be adopted by all health plans, clearinghouses, and providers that ensure the integrity and confidentiality of healthcare information. The security rule addresses healthcare information in all types of media instead of just electronic format. The final rule has an implementation date of April 2005.

(c) <u>National Identifier Codes</u>: Standards must be adopted by all health plans, clearinghouses, and providers regarding unique identifiers for providers, plans, employers, and individuals (beneficiaries). Presently, a final rule has been issued for the Employer ID. The Department of Health and Human Services has not published final rules for the remaining identifiers.

(d) <u>Enforcement</u>: The Office of Civil Rights has been appointed to enforce the privacy rule and has been given the authority to levy penalties for compliance failures. CMS has been designated to monitor the transaction and code sets compliance.

Although this Companion Guide deals with only one aspect of the entire "Administrative Simplification" provision, it is worth noting that all covered entities (health plans, clearinghouses, and providers) and their business partners are required to adhere to all aspects of the provision.

Section 1.09   HIPAA Internet Links

The following is a list of government agencies, industry leaders, and transaction and code set standards organizations associated with HIPAA. This is not an exhaustive list; however, each entity plays an integral role in the success of HIPAA and collective ly, represents a wealth of information that could not otherwise be included in our Companion Guide.

a) <u>Accredited Standards Committee (ASC X12)</u> - ASC X12 develops and maintains

standards for inter-industry electronic interchange of business transactions. http://www.x12.org/

b) American Dental Association (ADA) - The Dental Terminology 3rd and 4th Edition codes (CDT-4, HCPCS Level II "D" codes) and the Dental Content Committee that sets standards for the dental claim form and maintains dental codes can be linked from this site. http://www.ada.org

c) American Hospital Association Central Office on ICD-9-CM (AHA) - This site links to the International Classification of Diseases, Ninth Revision, Clinical Modification (ICD-9-CM) codes, used in medical transcription and billing, and for Level I HCPCS. www.ahacentraloffice.org

d) American Medical Association (AMA) - AMA owns the copyrights of the Current Procedural Terminology 4th Edition codes (CPT-4). http://www.ama-assn.org

e) Association for Electronic Health Care Transactions (AFEHCT) - A healthcare association dedicated to promoting the interchange of electronic healthcare information. http://www.afehct.org

f) Centers for Medicare and Medicaid Services (CMS) - Formerly known as HCFA, this site provides links to multiple web sites.

   i) The Electronic Health Care Transactions and Code Sets Model Compliance Plan - http://www.cms.gov/hipaa/hipaa3

   ii) The Healthcare Common Procedure Coding System (HCPCS) - http://cms.hhs.gov/medicare/hcpcs

   iii) For Medicaid HIPAA information related to the Administrative Simplification provision. http://www.cms.gov/medicaid/hipaa/adminsim

   iv) For HIPAA administrative simplification questions, CMS maintains an e-mail address at askhipaa@cms.hhs.gov and a toll free number at (866) 282-0659.

g) Designated Standard Maintenance Organizations (DSMO) - This site is a resource for information about the standard setting organizations, and transaction change request system. http://www.hipaa-dsmo.org

h) Health Level Seven (HL7) - HL7 is one of several ANSI accredited Standards Development Organizations (SDO), and is responsible for clinical and administrative data standards. http://www.hl7.org

i) Medicaid HIPAA Compliant Concept Model (MHCCM) - This site presents the Medicaid HIPAA Compliance Concept Model, information and a toolkit. http://www.mhccm.org

j) National Council of Prescription Drug Programs (NCPDP) - NCPDP is the standards and codes development organization for pharmacy. http://www.ncpdp.org

k) National Uniform Billing Committee (NUBC) - NUCB is affiliated with the American Hospital Association, and develops standards for institutional claims. http://www.nubc.org

l) National Uniform Claim Committee (NUCC) - NUCC is affiliated with the American Medical Association. It develops and maintains a standardized data set for use by the non-institutional health care organizations to transmit claims and encounter information. NUCC maintains the national provider taxonomy. http://www.nucc.org

m) Office for Civil Rights (OCR) - OCR is the Health and Human Services Office responsible for enforcing the Privacy Rule under HIPAA. http://www.hhs.gov/ocr/hipaa

n) For HIPAA privacy questions, OCR can be contacted at OCRPrivacy@hhs.gov or by calling (866) 627-7748.

o) United States Department of Health and Human Services (DHHS) - This site is a resource for the Notice of Proposed Rule Making, rules and other information regarding HIPAA. http://aspe.hhs.gov/admnsimp

p) Washington Publishing Company (WPC) - WPC is the official publisher for HIPAA transaction implementation guides and code sets. http://www.wpc-edi.com/hipaa

q) Workgroup for Electronic Data Interchange (WEDI) - A workgroup dedicated to improving healthcare through electronic commerce, which includes the Strategic National Implementation Process (SNIP) for complying with the administrative simplification provisions of HIPAA. http://www.wedi.org

Article II.   HIPAA Certification

Section 2.01   Certification Test Types

DCS will require each prospective electronic data interchange (EDI) submitter to be tested and approved before HIPAA transactions will be processed in production. The Workgroup for Electronic Data Interchange (WEDI), through a collaborative healthcare industry effort called the Strategic National Implementation Process (SNIP), has developed a White Paper entitled *Transaction Compliance and Certification*. This White Paper describes their recommended solutions for compliance testing and certification of HIPAA transactions and can be found at the following website: http://www.wedi.org/snip/public/articles/testing_whitepaper082602.pdf. The following highlight the seven types of testing described in this document:

a) Integrity Test: Testing of the EDI file for valid segments, segment order, element attributes, testing for numeric values in numeric data elements, validation of X12

syntax, and compliance with X12 rules. This will validate the basic level integrity of the EDI submission.

b) <u>Requirement Test</u>: Testing for HIPAA Implementation Guide-specific syntax requirements, such as repeat counts, used and not used codes, elements and segments, required or intra-segment situational data elements. Testing for non-medical code sets as laid out in the implementation guide. Values noted in the implementation guide via an X12 code list or table.

c) <u>Balance Test</u>: Testing the transaction for balanced field totals, financial balancing of claims or remittance advice, and balancing of summary fields, if appropriate.

d) <u>Situational Test</u>: Testing of specific inter-segment situations described in the HIPAA Implementation Guide, including the validation of situational fields based on rules present in the Implementation Guide for loops, segments, and data elements.

e) <u>External Code Set Test</u>: Testing for valid Implementation Guide-specific code set values. This type will not only validate the code sets but also make sure the usage is appropriate for any particular transaction.

f) <u>Specialty of Line of Business Test</u>: Testing to ensure that the segments and data elements required for certain healthcare services are present and correctly formatted according to the Implementation Guide.

g) <u>Trading Partner Requirements Test</u>: Testing to ensure that trading partner specific requirements are implemented.

Section 2.02   Certification Requirements

DCS will follow the WEDI/SNIP guidelines and require each prospective EDI submitter to certify their capability to produce transactions for the top six types of transaction testing. This certification must be obtained from a third party vendor (a list of known vendors is provided later in this section). DCS will obtain a third-party certification of our capability to produce compliant transactions. It is worth noting that some vendors have added the seventh type of testing that ensures the segments and data element requirements, specific to a trading partner (such as DCS) are present and correctly formatted. DCS will share our Companion Guide with any vendor willing to offer this seventh type of testing. Although DCS does not require certification of the seventh type at this time, it is definitely a benefit a submitter should consider when selecting a vendor for certification.

Certification for DCS is only required for the transactions that an organization is required or plans to conduct with DCS. Separate certification as appropriate will be required for the 837 Institutional and 837 Professional transactions. If your organization only does one type of the two 837 transactions, then certification for that transaction type, not all 837 transactions, is required. DCS is not interested in certification on transactions that are not appropriate for the Trading Partner relationship. Once a certification is validated,

the submitter is ready for type 7 testing and afterwards can be placed into production.

Section 2.03   Certification Vendors

As of the publication of this document, DCS is aware of the following vendors that offer HIPAA certification services:

Company; Internet Address; Telephone; Email Address

a) AppLabs Technologies; www.applabs.com; (215) 569-9976; info@applabs.net

b) Claredi; www.claredi.com; (801) 444-0339; info@claredi.com

c) Edifecs HIPAA-Desk; www.hipaadesk.com; (425) 250-0106; sales@edifecs.com

d) HIPAA Testing; www.hipaatesting.com; (480) 946-7200; info@hipaatesting.com

A submitter is not limited to these vendors in order to obtain the required certification. However, a submitter must be careful to select a vendor that offers a certification service, and not select a vendor that is limited to testing and validation services only. In addition, it is important that the vendor provide a certification for at least the top six types of transaction testing as previously discussed.

Article III.   Trading Partner Agreement

Section 3.01   General Overview

Each submitter will be required to complete a trading partner agreement (TPA). The TPA will be used to approve submitter identification information that is required on the HIPAA transactions. The first section of the TPA contains all of the HIPAA legal requirements. The next sections are forms used for specific transaction arrangements.

Section 3.02   DCS Electronic Data Interchange Request Form

The DCS HIPAA Electronic Data Interchange (EDI) Request Form is part of the TPA. The EDI Request Form is completed by the Trading Partner and provides a summary of the information exchanged between the Trading Partner and DCS. This form contains information about:

(a) Who is the contract entity?

(b) Who is authorized to add or change the data being provided or received or the users authorized to access the data?

(c) Who will be actually submitting the data, if different from the contracted entity?

(d) How the data exchange will occur (e.g., cartridge, FTP via VPN, Internet or e-mail)?

(e) Which transactions are intended for use between Trading Partner and DCS?

(f) Which transactions will generate a functional acknowledgement from the entity?

Article IV. Technical Environment

Section 4.01   DCS Communications Requirements

DCS intends on maintaining most of the current methods of communicating with DCS. These methods will include FTP, NDM, IBM tape cartridge, 3.5" diskette, and Compact Disc (CD). The primary method of connecting to the DCS network is by going from the Internet through a Virtual Private Network (VPN) tunnel to a secure FTP server. There are two types of VPN connections available:

(a) *Software-to-Hardware*. VPN client software is installed and configured on every machine at the client that requires FTP access.

(b) *Hardware-to-Hardware*. The client's network is interfaced with the DCS server allowing on-demand access to the FTP server.

Detailed VPN requirements can be obtained by contacting DCS. In general, these requirements include network interface card or modem, working Internet connection with a firewall, and installed VPN Client Software.

Section 4.02   File Encryption Procedures

Encryption is handled automatically as part of the creation of the VPN tunnel. The VPN client software on the user's computer or system will automatically de-encrypt the data after it reaches the user's system. All files and data that pass through the VPN tunnel are encrypted using at least a 128-bit algorithm.

Section 4.03   File and Directory Naming Conventions

The directory structure and file naming standards on the FTP server are designed to

provide logical access to all files, ease troubleshooting searches, and simplify security for account set ups and maintenance. DCS's FTP naming conventions for Trading Partners are as follows:

Filenames for HIPAA EDI transactions will be of the format **AAAABBBYYMMDDSS.EEE** where **AAAA** is encounter type, **BBB** is MCC number, **YYMMDD** is transmission date, **SS** is transmission sequence (starting at 01), and **EEE** is file format (txt or zip). The **AAAA** values reflecting the standard transaction type being transmitted and are r270 (**r**eceive), s271 (**s**olicited), u271 (**u**nsolicited), r276 (**r**eceive), s277 (**s**end), r278 (**r**eceive), s820 (**s**end), r834 (**r**eceive), s834 (**s**end), s835 (**s**end), d837 (**d**ental), i837 (**i**nstitutional), and p837 (**p**rofessional). For example, i83700303070401.zip is the first institutional 837 from MCC 003 sent on July 4, 2003 and the file is in a zip format.

The FTP directory names for Trading Partners during the test period prior to live transmission are \DCS\MCC###\in\editestI for inbound files and \DCS\MCC###\out\editestO for outbound files. The IP address is 10.170.9.6.

Standards for any other FTP submissions will be provided upon completion of the TPA.

Section 4.04 HIPAA Requirements

HIPAA standards are specified in the Implementation Guide (IG) for each transaction set and any authorized addenda. The guides include:

   (a) Format and contents of interchanges and functional groups,

   (b) Format and contents of the header, detailer and trailer segments specific to the transaction set,

   (c) Code sets and values authorized for use in the transaction set, and

   (d) Allowed exceptions to specific transaction set requirements.

Section 4.05 Multiple Transactions Within a File

DCS does not allow multiple transaction types to be submitted within a single file submission. While the X12 standards allow for multiple transaction set types such as an 837I, 837P, and 835 to be submitted within a single file, DCS does not support transaction bundling within a file. It is thought that this limitation provides for a "cleaner" processing environment.

Section 4.06 Size of Transmissions/Batches

Transmission sizes are limited based upon the number of Segments/Records allowed by HIPAA standards. HIPAA standards for the maximum file size of each transaction set are specified in the appropriate Implementation Guide or its authorized addenda.

DCS file transfer limits set within DCS may be larger than the recommendations in the Implementation Guides. For 837 transactions, the limit is 250,000 claim encounters. There is no limit on the 270, 271 transaction file sizes.

Section 4.07   Complete Transmission Check

All transactions are checked to ensure that the transmission is complete. The transaction header and footer must balance before a transaction file is processed.

Section 4.08   Balancing Data Elements

DCS will utilize any balancing requirements that can be derived from the transaction implementation guides. All financial amount fields must be balanced at all levels available within the transaction set. The number of transactions in the header and footer must equal and be the same as the number of transactions in the file.

Article V.   Testing Procedures

Section 5.01   Testing Requirements

DCS will require internal testing with all of its trading partners before a transaction is placed into production. Any submitter is welcome to request internal testing once HIPAA certification is presented to and validated by DCS. Many details of the internal testing process and how to notify DCS of HIPAA certification not contained in this document are part of the TPA. DCS offers internal testing with our Trading Partners as a means to test our Companion Guide requirements. However, DCS maintains a third-party certification of our capability to produce compliant transactions.

DCS reserves the right to discontinue any internal testing with any submitter if DCS determines that errors, which should have been corrected by the submitter as part of their certification process are present. DCS currently offers full production volume testing, as part of internal testing. Upon request, DCS will make available sample transaction files. Follow the contact information in section 1.04 to request sample files.

DCS expects each individual Trading Partner to be responsible for ensuring that its transactions are compliant. Compliance includes both the HIPAA mandates and DCS Trading Partner requirements contained in the Companion Guide.

Compliance testing should include the internal validation of all used transaction sets. Plus, DCS requires Trading Partners to use a neutral third party tool/vendor to certify that the Trading Partner can produce and accept HIPAA compliant transaction sets. This tool/vendor should provide certification through type 6 compliance testing as outlined by the WEDI/SNIP guidelines.

After a Trading Partner has type 1 through type 6 certification, DCS and the Trading Partner will begin more specific transaction testing to ensure testing type 7 compliance. This type of testing will ensure that files can be passed between DCS and our trading partner without truncation or distortion of the data on the file.

All of the specifications for type 7 testing can be found in the Companion Guide documents. Any additional specific procedures for testing will be provided to the Trading Partner in a stand-alone memorandum immediately prior to the start of testing for a transaction set.

Section 5.02   Test Data

DCS believes that, where possible, using "real" data will enhance the overall value of the compliance testing process. However, if the Trading Partner elects to do so it must ensure that it remains in compliance with all Federal and state privacy regulations. In particular, DCS expects that Patient Identifiable Information will be encrypted or eliminated from tests submitted to the certification testing system unless the testing system is in compliance with all HIPAA regulations concerning security, privacy, and business associate agreements.

Section 5.03   Testing Procedures

Testing procedures may be provided to the Trading Partner in a stand-alone memorandum immediately prior to the start of testing for a given transaction set.

Article VI. Acknowledgment Processes

Section 6.01   Overview of Acknowledgment Processes

Acknowledgment transactions let the sender know that the receiver received their transactions and that the transactions were accepted with no errors, accepted with errors, or rejected. The two types of Acknowledgment Transactions available are the:

(a) Interchange (TA1) Acknowledgment

(b) Functional Acknowledgment Transaction Set (997).

Section 6.02   DCS Requirements

(a) DCS plans on using the 997 transaction to acknowledge all files received by DCS.

(b) A Trading Partner may elect to send DCS an acknowledgement on any or all addition files. These acknowledgements should be listed on the EDI Request Form.

Section 6.03   997 Functional Acknowledgment Transaction Sets

The 997 Functional Acknowledgment Transaction (997 Transaction) is designed to check each functional group in an interchange for data and syntax errors and send the results back to the sending Trading Partner. The 997 transaction can accept or reject records at the functional group, transaction set, segment or data element level. The HIPAA statute and current implementation guides do not mandate the use of the 997 transaction but recommended its usage. Characteristics of the 997 transaction include:

(a) One 997 transaction corresponds to one functional group in the interchange.

(b) 997 transactions are transaction sets and thus are included in the interchange control structure (envelopes) for transmission.

(c) Many commercially available translators can automatically reconcile the 997 transaction back to the previously sent functional group. This process allows the sending Trading Partner to identify any transaction sets that have not been acknowledged by the receiving Trading Partner.

997 transactions should not be used to acknowledge the receipt of other 997 transactions. Details on the format and syntax of the 997 transaction can be found in Appendix B of the Transaction Set's Standard Implementation Guide.

Section 6.04   Rejected Transmissions and Transactions

The process for handling rejected transactions and transmissions will vary based on the error(s) causing the rejection.

(a) Interchanges or functional groups may be completely rejected for IG format violations.

(b) Individual records or transaction sets within a functional group/interchange will be rejected only in Fee-For-Service files.

(c) Rejection of encounter data will be done at the file level.

Numerous edits will be performed on each transaction processed. Each of these edits has a severity level associated with it that in conjunction with the number of errors will determine accept/reject status.

Article VII. HIPAA Glossary

See website http://www.wedi.org/public/articles/HIPAA_glossary.pdf for a glossary of common HIPAA terms.